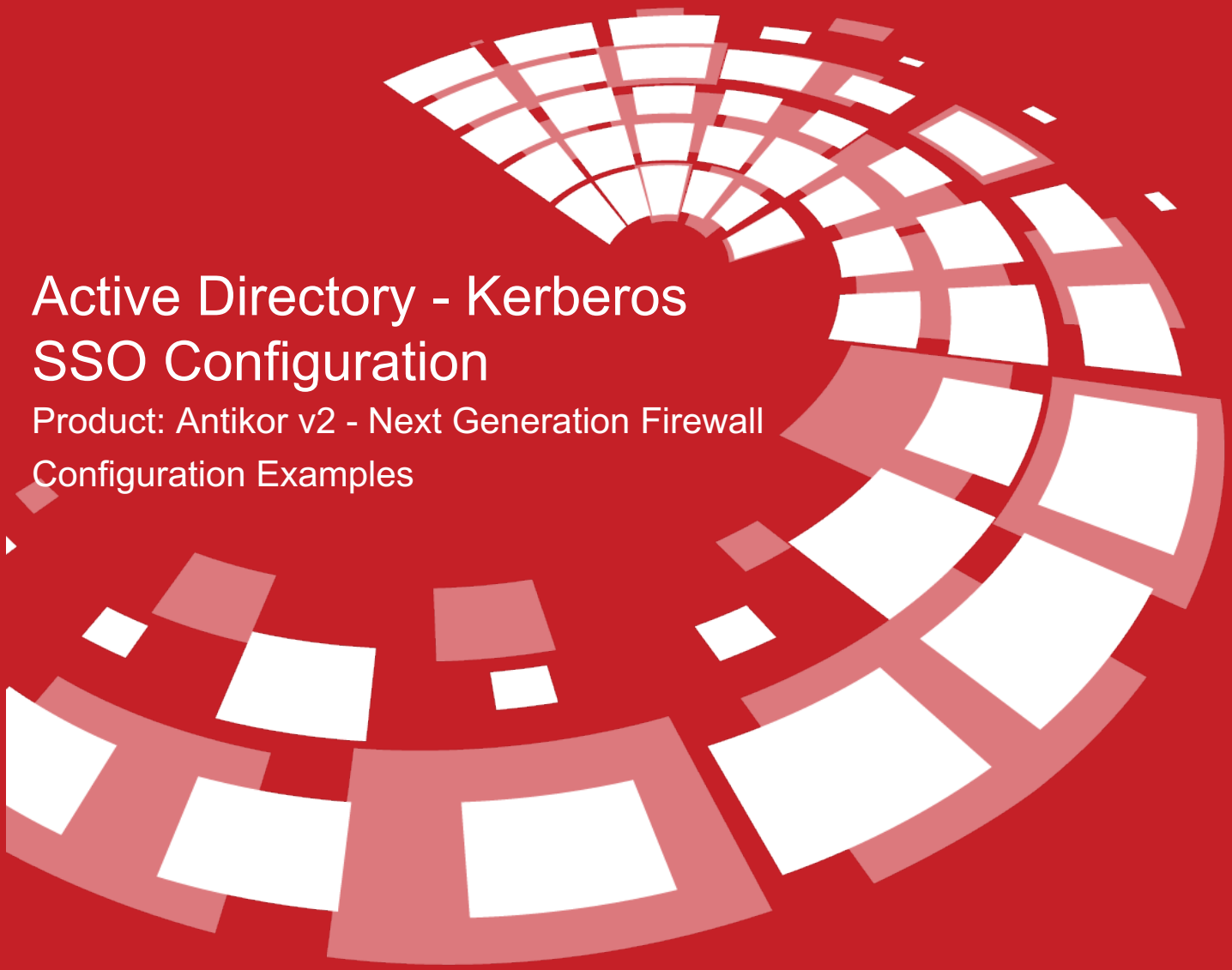
epati

Active Directory - Kerberos SSO Configuration

Product: Antikor v2 - Next Generation Firewall

Configuration Examples



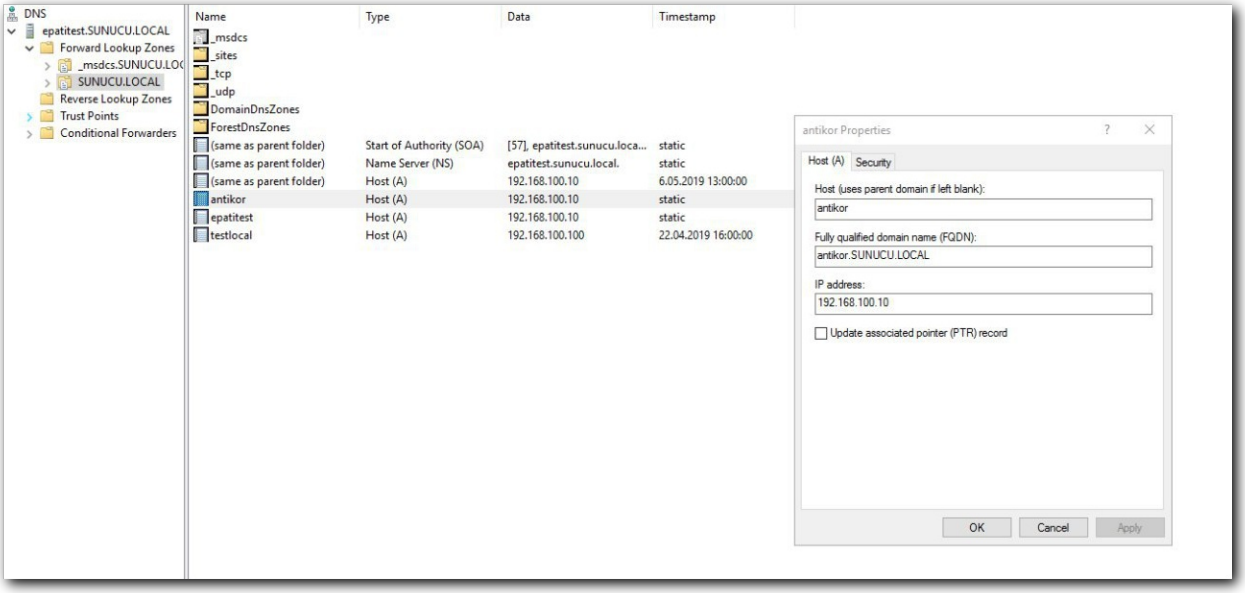
www.epati.com.tr

Active Directory - Kerberos SSO Configuration

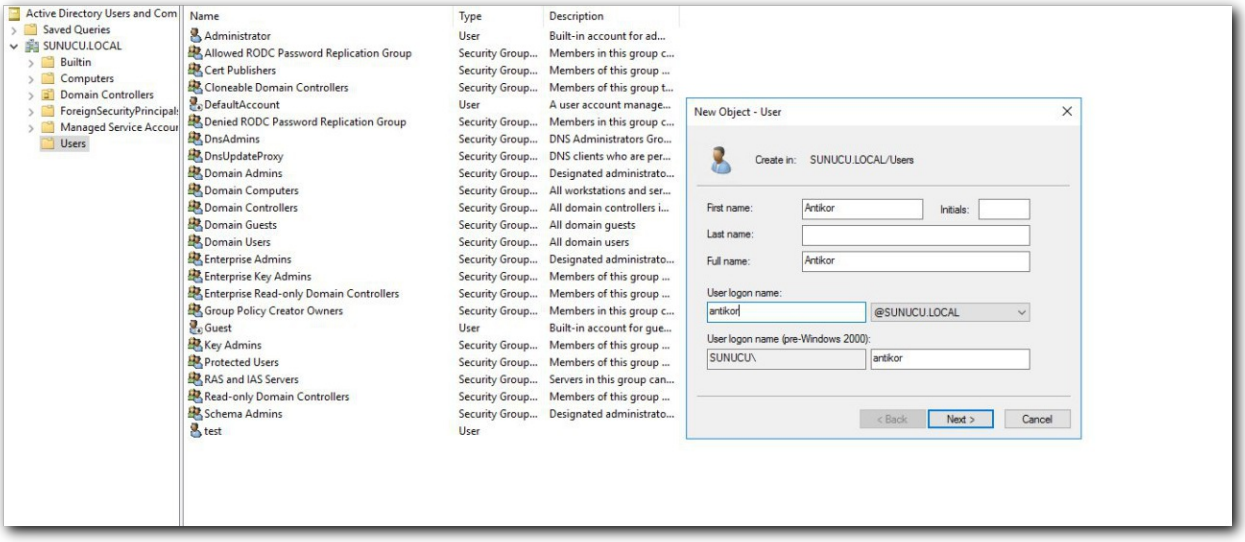
Kerberos is an authentication protocol developed to prove the identity of resources that communicate on the network. SSO (Single Sign On) provides access by logging in with a single user ID.

Things to do on the Active Directory

1. A record must be entered on the DNS server in Domain Controller.



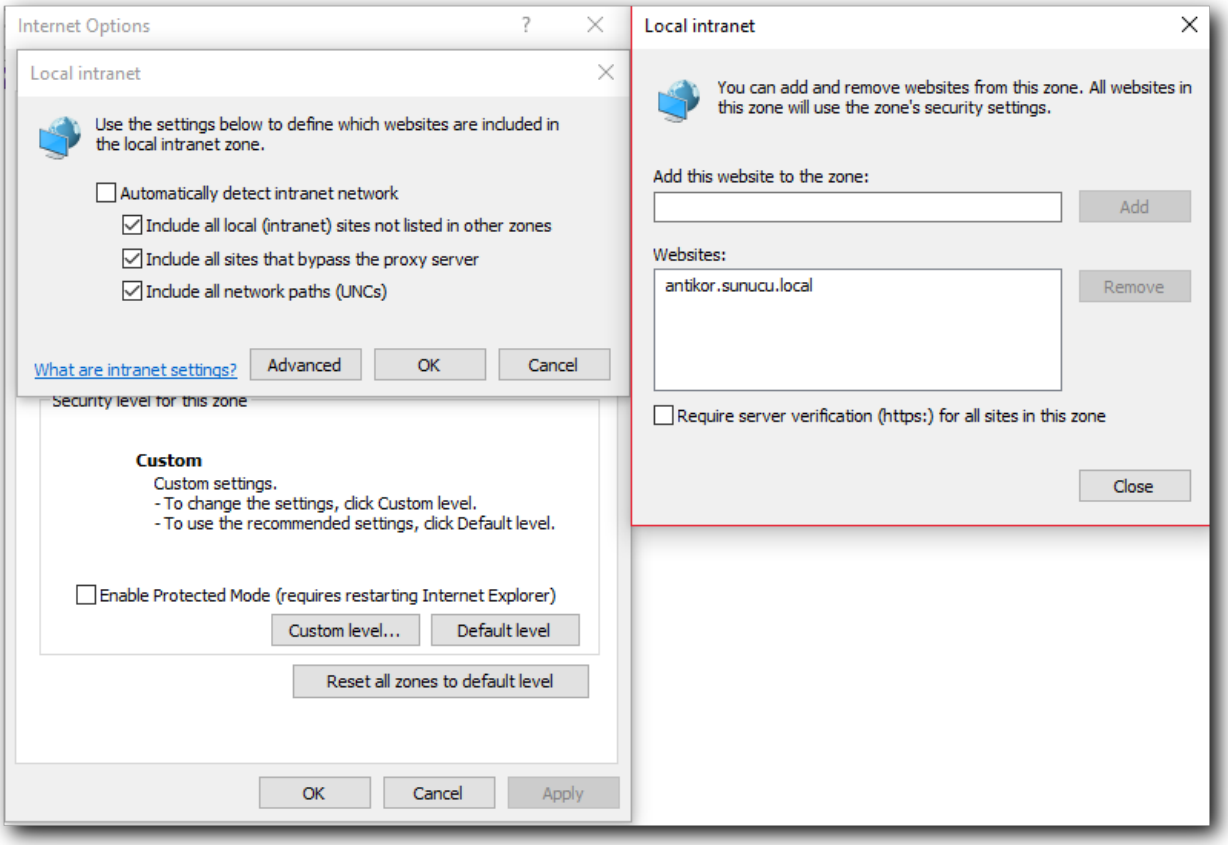
2. The a user named Antikor must be created in the Domain Controller.



3. The CMD should be opened as an administrator and the keytab file should be created with the following command.

```
ktpass -princ HTTP/antikor.SUNUCU.LOCAL@SUNUCU.LOCAL -mapuser antikor@SUNUCU.LOCAL -crypto al
-ptype KRB5_NT_PRINCIPAL -pass SIFRE -out antikor.krb.keytab
```

4. antikor.SUNUCU.LOCAL should be written in the Internet Explorer > Security > Local Intranet > Sites > Advanced .

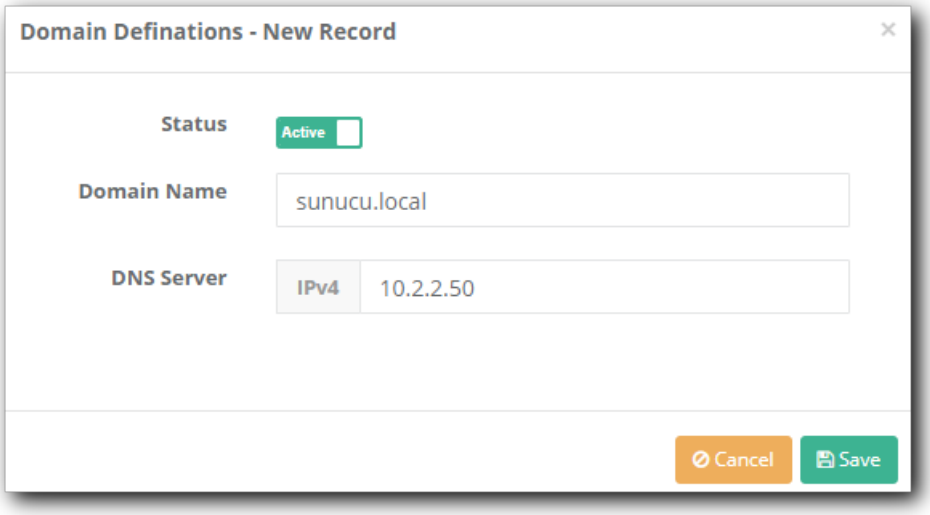


5. The Antikor SSL certificate must be distributed with Group Policy settings to all clients.

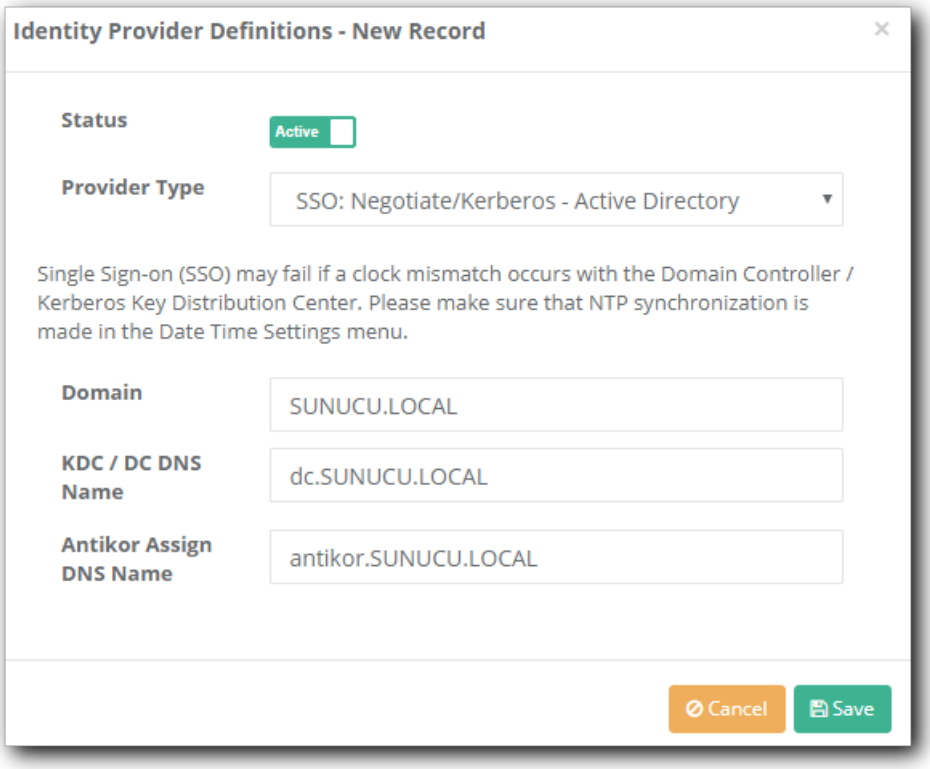
To add trusted sites using a GPO (Group Policy Objects), Launch Active Directory Users and Computers (ADUC), right click on the domain the clients are in, select Properties > Group Policy > New, type in a name for the GPO (like “IE Security Settings”) and then select Edit > User Configuration > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings. Select Import the current security zones and privacy settings > Modify Settings > Trusted Sites > Sites and add your Plexcel protected websites just as you would on a client. Then wait for the policy to propagate throughout the domain.

Things to do on the Antikor

1. The SUNUCU
.LOCAL record is must created on the Antikor Domain Definitions page.

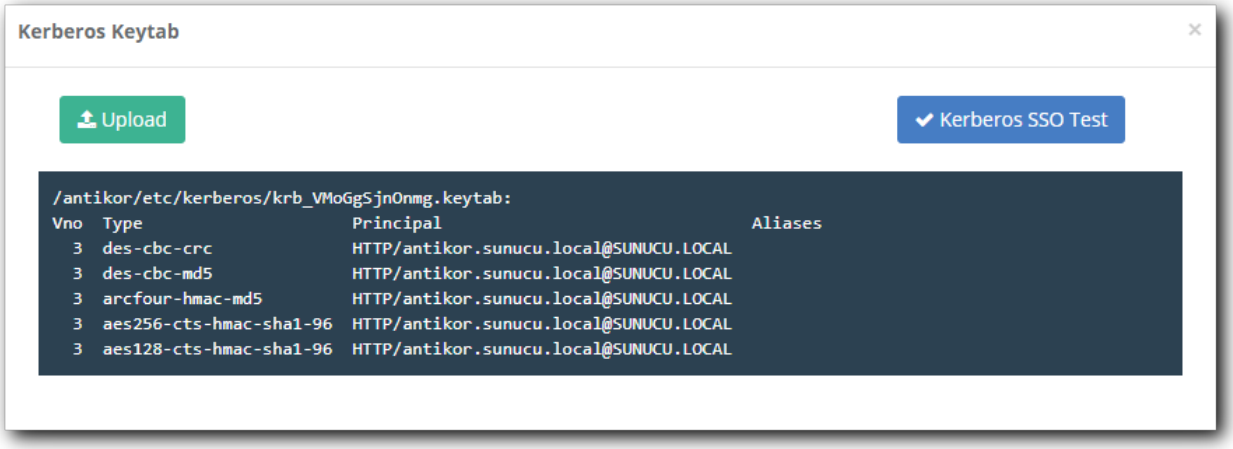


2. Enter the record by selecting Provider Type SSO: Negotiate / Kerberos - Active Directory on the Identity Provider Definitions page.



3. The generated Keytab file will be uploaded via the Upload button. The Root Certificate button will appear if the “Single Sign-On SSO” option is enabled on the Verification Rules page.

When the Keytab file is loaded information like the following will appear;



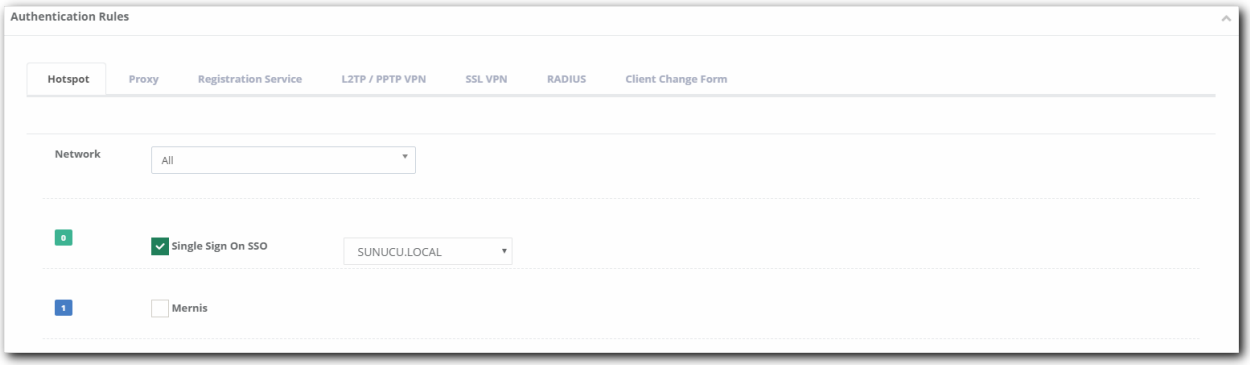
The Kerberos SSO Test button can be used for testing.

4. Once all the steps have been performed, the login process will be performed successfully.

Points to consider on the Antikor

1. NTP Server must be set.

2. The Single Sign-On SSO feature must be enabled on the Hotspot tab on the Verification Rules page..



3. The date / time settings for the Domain Server, Client and Antikor must be the same.

4. IP addresses/IP block for SSO authentication should be added to on the Hotspot Clients page.